Configurare TLSv1.3 per Secure Email Web Manager

Sommario

Introduzione

Questo documento descrive la configurazione del protocollo TLS v1.3 per Cisco Secure Email e Web Manager (EWM)

Prerequisiti

È necessario avere una conoscenza generale delle impostazioni e della configurazione di SEWM.

Componenti usati

- Cisco Secure Email Web Manager (SEWM) AsyncOS 15.5.1 e versioni successive.
- Impostazioni di configurazione SSL.

"Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi".

Panoramica

Il SEWM ha integrato il protocollo TLS v1.3 per crittografare le comunicazioni per i servizi correlati a HTTPS; interfaccia utente classica, NGUI e API Rest.

Il protocollo TLS v1.3 offre una comunicazione più sicura e una negoziazione più rapida, in quanto il settore si impegna a farne il protocollo lo standard.

SEWM utilizza il metodo di configurazione SSL esistente all'interno di SEGWebUI o CLI di SSL con alcune impostazioni importanti da evidenziare.

- Consigli cautelativi per la configurazione dei protocolli autorizzati.
- I cifrari TLS v1.3 non possono essere manipolati.
- TLS v1.3 può essere configurato solo per GUI HTTPS.
- Le opzioni di selezione della casella di controllo del protocollo TLS tra TLS v1.0 e TLS v1.3 utilizzano uno schema illustrato più dettagliatamente all'interno dell'articolo.

Configurazione

Il servizio SEWM ha integrato il protocollo TLS v1.3 per HTTPS in AsycOS 15.5.

È consigliabile prestare attenzione quando si scelgono le impostazioni del protocollo per evitare errori HTTPS.

Il supporto del browser Web per TLS v1.3 è comune, anche se alcuni ambienti richiedono delle regolazioni per accedere a SEWM.

L'implementazione SEWM di Cisco del protocollo TLS v1.3 supporta 3 cifrari predefiniti che non possono essere modificati o esclusi all'interno del SEWM.

Cifre TLS 1.3:

TLS_AES_256_GCM_SHA384

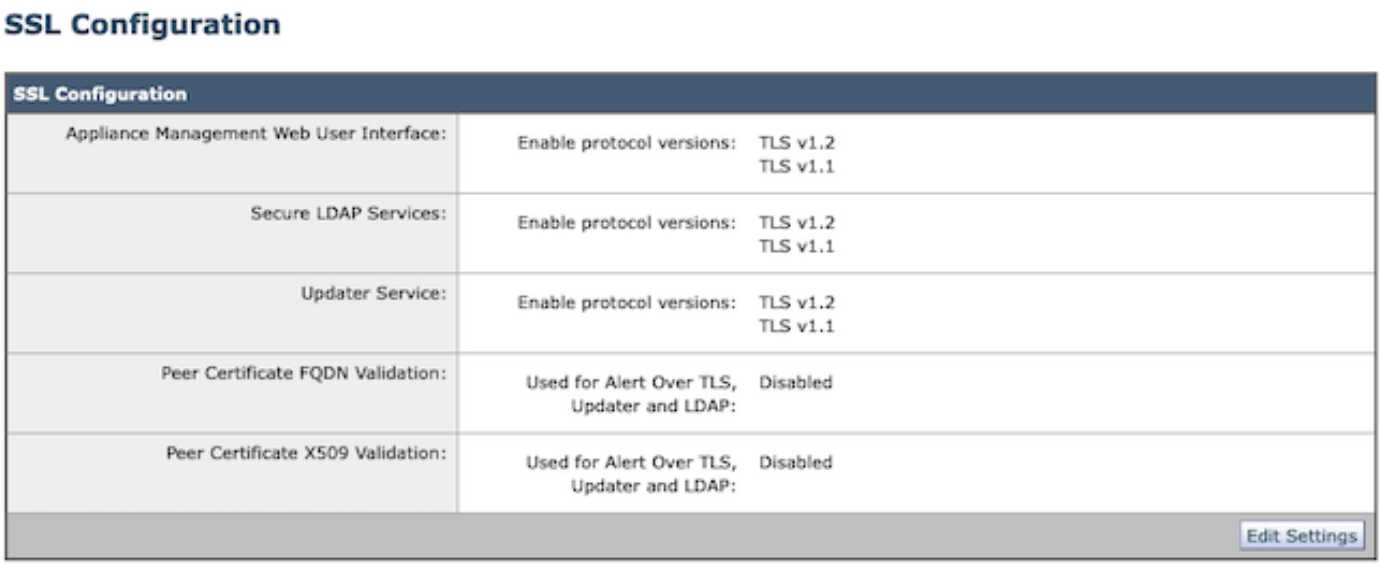
TLS_CHACHA20_POLY1305_SHA256

TLS_AES_128_GCM_SHA256

Configurazione da WebUI

Selezionare > Amministrazione sistema > Configurazione SSL

- Dopo l'aggiornamento a 15.5 AsyncOS HTTPS, la selezione del protocollo TLS predefinito include solo TLS v1.1 e TLS v1.2.
- I due servizi aggiuntivi elencati, Servizi LDAP sicuri e Servizi di aggiornamento, non supportano TLS v1.3.

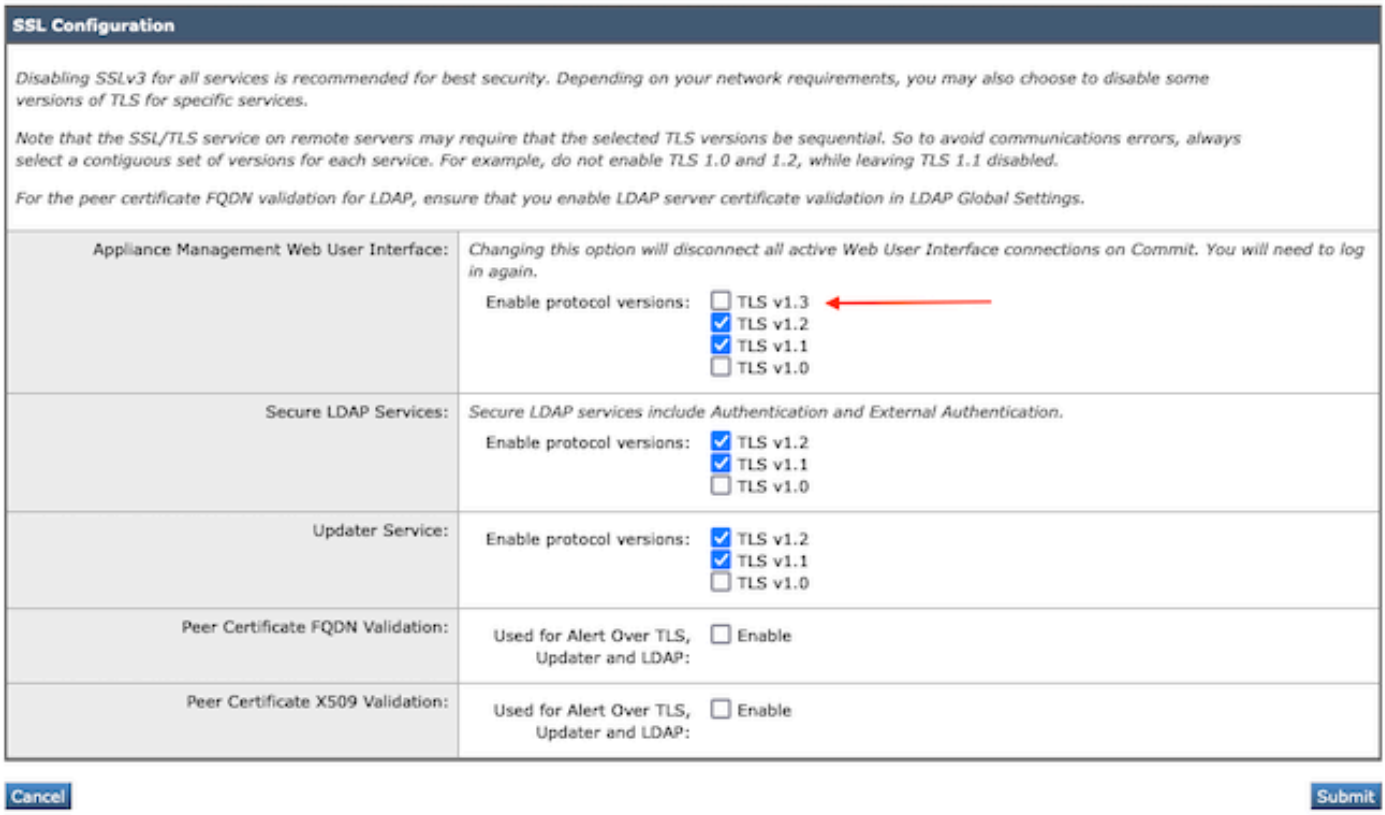


Selezionare "Edit Settings" (Modifica impostazioni) per visualizzare le opzioni di configurazione.

Le opzioni di selezione del protocollo TLS per "Web User Interface" includono TLS v1.0, TLS v1.1,

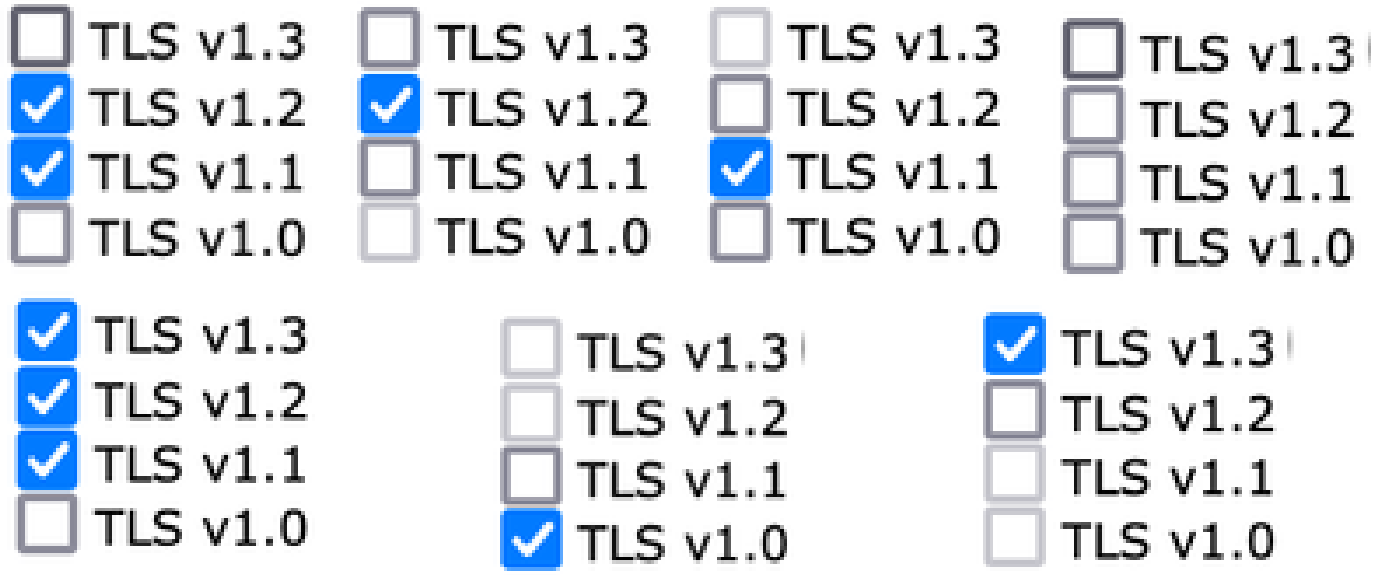
TLS v1.2 e TLS v1.3.

- Dopo l'aggiornamento ad AsyncOS 15.5, per impostazione predefinita vengono selezionati solo i protocolli TLS v1.1 e TLS v1.2.

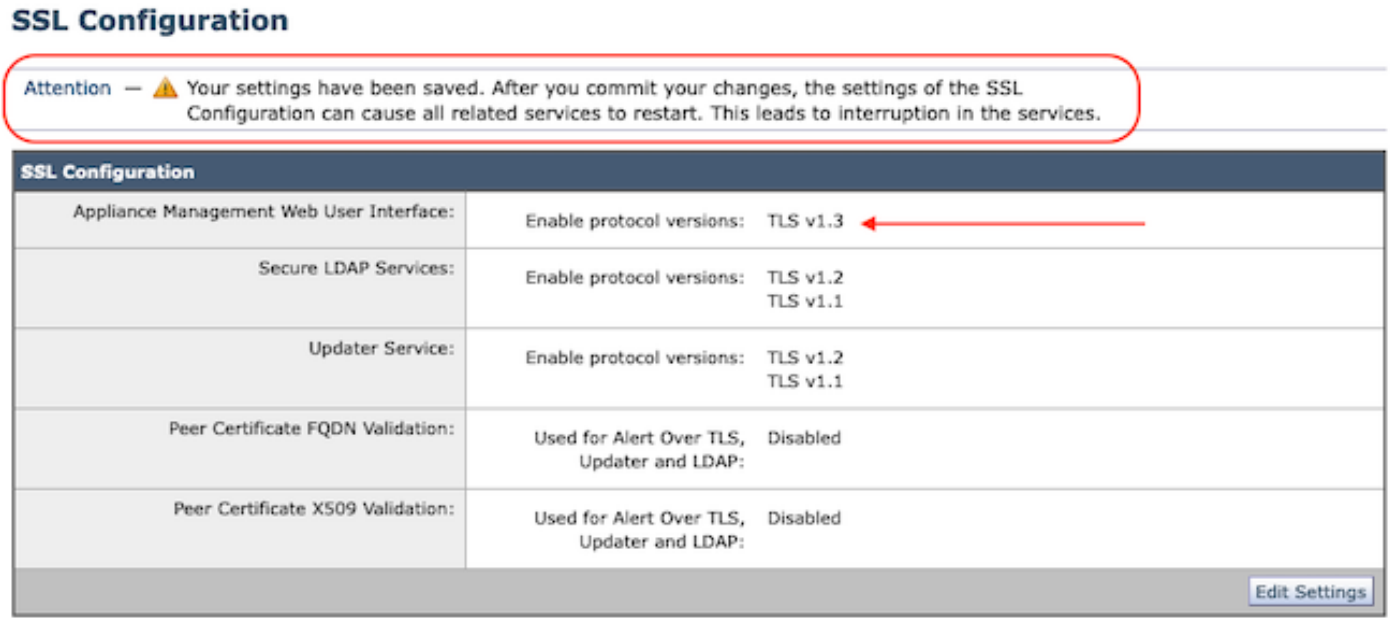


Nota: TLS1.0 è deprecato e quindi disabilitato per impostazione predefinita. TLS v1.0 è ancora disponibile se il proprietario sceglie di attivarlo.

- Le opzioni della casella di controllo si illuminano con caselle in grassetto che presentano le caselle Protocolli disponibili e In grigio per le opzioni non compatibili.
- Le opzioni di esempio nell'immagine illustrano le opzioni delle caselle di controllo per l'interfaccia utente Web.



Nota: le modifiche apportate alla configurazione SSL possono causare il riavvio dei servizi correlati e causare una breve interruzione del servizio WebUI.



Configurazione dalla CLI

EWM consente TLS v1.3 su un servizio: WebUI

sma1.example.com> sslconfig

Per una protezione ottimale, è consigliabile disattivare SSLv3.

Il servizio SSL/TLS sui server remoti richiede che le versioni TLS selezionate siano sequenziali. Per evitare errori di comunicazione, selezionare sempre un
set di versioni per ogni servizio. Ad esempio, non abilitare TLS 1.0 e 1.2, lasciando TLS 1.1 disabilitato.

Scegliere l'operazione da eseguire:
- VERSIONS - Abilita o disabilita le versioni SSL/TLS
- PEER_CERT_FQDN - Convalida la conformità FQDN del certificato peer per Alert over TLS, Updater e LDAP.
- PEER_CERT_X509 - Convalida della conformità X509 dei certificati peer per Alert Over TLS, Updater e LDAP.
[]> versioni

Abilitare o disabilitare la versione SSL/TLS per i servizi:

Programma di aggiornamento - Servizio di aggiornamento
WebUI - Interfaccia utente Web di Gestione accessorio
LDAPS - Servizi LDAP sicuri (incluse autenticazione e autenticazione esterna)

TLSv1.3 non è disponibile per Updater e LDAPS. Solo WebUI può essere configurato con TLSv1.3.

Versioni SSL/TLS attualmente abilitate per servizio: (S : Abilitato, N : Disabilitato)

	Aggiornamento	LDAP	WebUI
TLSv1.0	N	N	
TLSv1.1	Y	N	Y
TLSv1.2	Y		Y
TLSv1.3	N/D		N/D

Selezionare il servizio per il quale abilitare/disabilitare le versioni SSL/TLS:

1. Programma di aggiornamento
2. Interfaccia Web
3. LDAPS
4. Tutti i servizi
[]> 2

I protocolli attualmente abilitati per WebUI sono TLSv1.2.

Per modificare l'impostazione di un protocollo specifico, selezionare una delle seguenti opzioni:

1. TLSv1.0
2. TLSv1.1
3. TLSv1.2
4. TLSv1.3
[]> 4

Il supporto TLSv1.3 per l'interfaccia utente Web di gestione dell'accessorio è attualmente disattivato. Abilitarlo? [N]> y

I protocolli attualmente abilitati per WebUI sono TLSv1.3, TLSv1.2.

Scegliere l'operazione da eseguire:
- VERSIONS - Abilita o disabilita le versioni SSL/TLS
- PEER_CERT_FQDN - Convalida la conformità FQDN del certificato peer per Alert over TLS, Updater e LDAP.
- PEER_CERT_X509 - Convalida della conformità X509 dei certificati peer per Alert Over TLS, Updater e LDAP.
[]>

sma1.example.com> esegui

Avviso: le modifiche apportate alla configurazione SSL causano
questi processi da riavviare dopo Commit - gui,euq_webui.
Ciò provoca una breve interruzione delle operazioni SMA.

Immettere alcuni commenti che descrivono le modifiche:
[]> abilitazione di tls v1.3

Modifiche approvate: Sun gen 28 23:55:40 2024 EST
Riavvio dell'interfaccia utente in corso...
interfaccia utente riavviata
Riavvio di euq_webui...
euq_webui riavviato

Attendere qualche istante e verificare che WebUI sia accessibile.

Nota: se si selezionano più versioni di TLS per un servizio, è necessario che l'utente selezioni un servizio e una versione del protocollo, quindi ripeta la selezione di un servizio e di un protocollo fino a quando tutte le impostazioni non sono state modificate.

Verifica

In questa sezione sono inclusi alcuni scenari di test di base e gli errori che possono verificarsi a causa di versioni non corrispondenti o errori di sintassi.

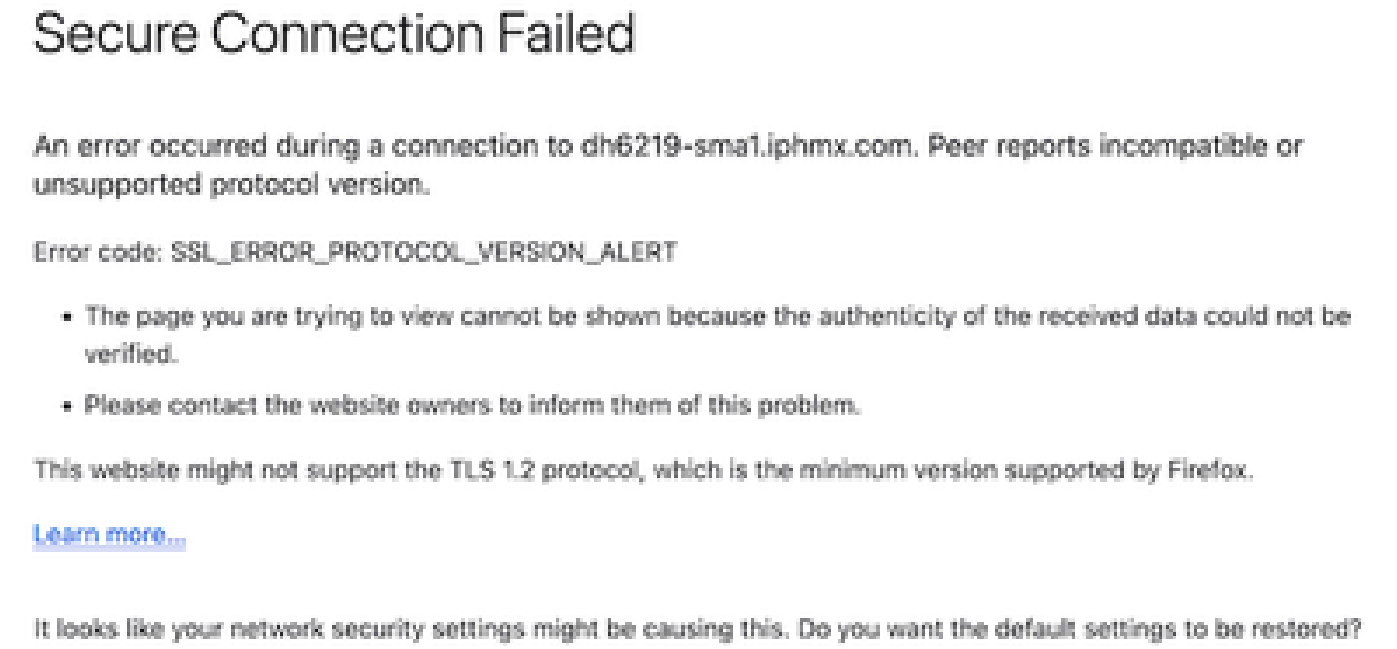
Verificare la funzionalità del browser aprendo una sessione del browser Web su EWM WebUI o NGUI configurato con TLSv1.3.

Tutti i browser Web testati sono già configurati per accettare TLS v1.3.

- Esempio di impostazione del browser su Firefox per disattivare il supporto di TLS v1.3 si verificano errori sia sull'interfaccia ClassicUI che sull'interfaccia NGUI dell'accessorio.

- Interfaccia utente classica che utilizza Firefox configurata per escludere TLS v1.3 come test.
- NGUI riceverà lo stesso errore con l'unica eccezione del numero di porta 4431 (predefinito)

all'interno dell'URL.



Errore TLS v1.3 Webui

- Verificare le impostazioni del browser per assicurarsi che TLSv1.3 sia incluso. (Questo esempio viene da Firefox)

- Il comando openssl di esempio che utilizza un valore di cifratura digitato in modo errato restituisce il seguente output dell'errore: sample openssl connection test failure due to invalid cipher: Error with command: "-ciphersuites TLS_AES_256_GCM_SHA386"

2226823168:ERROR:1426E089:SSL routine:ciphersuite_cb:no cipher match:ssl/ssl_ciph.c:1299:

- Questo errore viene generato dal comando arricciato di esempio eseguito su ng-ui quando TLS v1.3 è disabilitato.

curl: (35) CURL_SSLVERSION_MAX incompatibile con CURL_SSLVERSION

Informazioni correlate

- Cisco Content Security Management Appliance - Note sulla release
- Cisco Content Security Management Appliance - Guide per l'utente

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).